

AMENDMENTS TO THE CLAIMS:

This listing of claims will replace all prior versions, and listings, of claims in the application:

LISTING OF CLAIMS:

1. (Currently Amended) A process to identify a user terminal resource or a user of the terminal resource by a server resource in a telecommunication network, using a first identifier, where an asymmetrical algorithm with public key ~~[[is]]~~ and a symmetric algorithm are implemented in the terminal resource, comprising the following steps:

generating a random number in the user terminal resource,

determining in the terminal resource a second identifier as a function of the random number, at least from part of the first identifier and from the result of executing the asymmetrical algorithm and the symmetrical algorithm, wherein to ~~which~~ at least the random number is applied to both algorithms,

transmitting the second identifier to the server resource, and

in the server resource, retrieving the first identifier at least by executing the asymmetrical algorithm to which a private key and, at least partially, the second identifier are applied, so that the server resource verifies that the first retrieved identifier is written into a memory of the server resource.

2. (Previously Presented) A process according to claim 1, further including the step of authenticating the terminal resource by the server resource subsequent to the steps of claim 1.

3. (Previously Presented) A process to identify a user terminal resource or a user of the terminal resource by a server resource in a telecommunication network, using a first identifier, where an asymmetrical algorithm with public key is implemented in the terminal resource, comprising the following steps:

generating a random number in the user terminal resource;

determining in the terminal resource a second identifier as a function of the random number, wherein the determination in the terminal resource includes application of the generated random number to the asymmetrical algorithm with the public key to produce an encrypted random number, application of the generated random number and the first identifier to a symmetrical algorithm implemented in the terminal resource, to produce an encrypted identifier, and concatenation of the encrypted random number and of the encrypted identifier in the second identifier;

transmitting the second identifier to the server resource; and

in the server resource, retrieving the first identifier, wherein the retrieval in the server resource includes application of the encrypted random number to the asymmetrical algorithm with the private key, in order to retrieve the generated random number, and application of the retrieved random number and the encrypted identifier to the symmetrical algorithm, in order to retrieve the first identifier so that the server resource verifies that the first retrieved identifier is stored in a memory of the server resource.

4. (Currently Amended) A process to identify a user terminal resource or a user of the terminal resource by a server resource in a telecommunication network,

using a first identifier, where an asymmetrical algorithm with public key [[is]] and a symmetrical algorithm are implemented in the terminal resource, comprising the following steps:

generating a random number in the user terminal resource;

determining in the terminal resource a second identifier as a function of the random number, wherein the determination in the terminal resource includes application of the generated random number ~~concatenated to the first identifier~~, to the asymmetrical algorithm with the public key and to a symmetric algorithm with the first identifier to produce the second identifier;

transmitting the second identifier to the server resource; and

in the server resource, retrieving the first identifier, wherein the retrieval in the server resource includes application of the second identifier to the asymmetrical algorithm with the private key in order to retrieve the first identifier so that the server resource verifies that the first retrieved identifier is stored in a memory of the server resource.

5. (Previously Presented) A process according to claim 1, further including the steps of changing the public key and the private key for the asymmetrical algorithm in the server resource, and downloading the changed public key from the server resource to the terminal resource.

6. (Previously Presented) A process according to claim 1, wherein the generation of the random number is periodic in the terminal resource.

7. (Previously Presented) A process according to claim 1, wherein the generation of the random number occurs following at least one of the following events in the terminal resource: switching on the terminal resource, setting-up a call, setting-up a session between the terminal resource and the server resource, substitution of the server resource for another server resource, or activation of a service application.

8. (Currently Amended) A user terminal resource identifying itself, or identifying a user of the latter, to a server resource, through a telecommunication network, using a first identifier, an asymmetrical algorithm with a public [[key]] key, and a symmetric algorithm implemented in the terminal resource, comprising:

- a resource to generate a random number, and
- a resource to determine a second identifier as a function of the random number, at least from part of the first identifier and from the result of executing the asymmetrical algorithm and the symmetric algorithm to which at least the random number is applied to both algorithms in order to transmit the second identifier to the server resource, which retrieves the first identifier at least by executing the asymmetrical algorithm to which a private key and, at least partially, the second identifier are applied, and which verifies that the first retrieved identifier is written into a memory of the server resource.

9. (Previously Presented) A user terminal resource according to claim 8, wherein the resource to generate a random number and the resource to determine a second identifier are included in a portable electronic object of the chip card type.

10. (Currently Amended) A method for identifying at least one of a terminal and a user of the terminal to a server in a telecommunications network, comprising the following steps:

generating a random number in the terminal;

applying said random number and a first identifier associated with said terminal to at least one asymmetric algorithm and at least said random number to a symmetric algorithm in said terminal, using a public key, to generate a second identifier that is based upon a combination of said random number and said first identifier;

transmitting said second identifier to said server;

applying a portion of said second identifier to said asymmetric algorithm and said symmetric algorithm in said server, using a private key, to derive said first identifier; and

authenticating said terminal or said user in the server, using the derived first identifier.

11. (Currently Amended) The method of claim 10, wherein said random number is applied to said asymmetric algorithm in said terminal, together with said public key, to generate a first result, and said first identifier is applied to ~~a second, different~~ said symmetric algorithm in said terminal, together with a key, to generate a second result, and wherein said second identifier comprises a combination of said first and second results.

12. (Canceled)

13. (Previously Presented) The method of claim 11, wherein said second identifier comprises a concatenation of said first and second results.

14. (Previously Presented) The method of claim 10, wherein said random number is combined with said first identifier, and the combination of said random number and said first identifier is applied as an input to said asymmetric algorithm in said terminal, together with said public key, to generate said second identifier.

15. (Previously Presented) The method of claim 14, wherein said combination comprises a concatenation of said random number and said first identifier.

16. (New) The process of claim 1, in the server resource, further comprising:
applying the random number to an asymmetric algorithm to produce an
identity of the terminal resource,

wherein executing the asymmetrical algorithm produces the random number.